UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
WESTERN DIVISION
Case No. 3:22MJ5044

AFFIDAVIT TO COMPLAINT

I, Alex O. Hunt, being duly sworn and deposed, states the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am an "investigative or law enforcement officer of the United States" empowered to make arrests within the meaning of Title 18, United States Code, Section 3052 and to execute search warrants and conduct seizures within the meaning of Title 18, United States Code, Section 3107 for violations of the laws of the United States.

2. I am a duly appointed Special Agent, employed by the United States Department of Justice, Federal Bureau of Investigation (FBI). I have been a Special Agent with the FBI since 2015. I am currently assigned to the FBI Cleveland Division, Toledo Resident Agency. I was previously employed as a patrol officer and as a criminal investigator in Gwinnett County, Georgia from 2009 to 2015. Since 2009, I have received training and have experience in interviewing and interrogation techniques, arrest procedures, search and seizure, search warrant applications, and various other crimes and investigation techniques.

3. This affidavit is submitted in support of a criminal complaint to arrest ZACHARY RYAN BALUSIK (hereinafter "BALUSIK") for violations of 18 U.S.C. §§ 2252(a)(4)(B), Possession of and/or Access with Intent to View Child Pornography, and 2252(a)(2), Receipt and/or Distribution of Child Pornography. All of the information contained in this affidavit is the result of either my personal observations and investigation or has been provided to me by other law enforcement officers, all of whom I believe are reliable. This affidavit contains

information to establish probable cause for a criminal complaint, and thus, does not list every fact known in the investigation.

PROBABLE CAUSE

4. On or about March 29, 2021, an FBI Online Covert Employee ("OCE") was connected to the Internet in an online undercover capacity and accessed an online chatting application (the "Chat Application").[1] The Chat Application is a free mobile application that can be downloaded on desktop computers and mobile devices, including Apple iOS and Android devices. It permits users to anonymously send text messages, videos, images, and other content using end-to-end encryption. The Chat Application allows users to create groups to exchange messages and files with other users of the application.

5. While using this Chat Application, the OCE infiltrated various groups that were dedicated to child pornography, also known as "child sexual abuse material" or "CSAM." One such group on the Chat Application was titled, "Nepirape." The term "nepi," as used by child sex offenders or CSAM consumers, refers to a sexual interest in infants and toddlers. This group was dedicated to sharing CSAM of children 4 years of age or younger. The group had the following description under its name "Only 0 to 4."

6. The OCE observed numerous CSAM files being shared by users in this group. Around March 29, 2021, the OCE observed a user in the group share a link for a meeting (the

[1] The identity of the Chat Application is not disclosed herein to protect an on-going investigation. This application remains active and disclosure of the name of the application would potentially alert its users to the fact that law enforcement action is being taken against users of the application, thereby provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, to protect the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the application will be identified herein as the "Chat Application."

"Subject Meeting") on an Internet-based video conferencing application. This application is hereinafter referred to as "Application A."[2]

7. "Application A" is designed for video conferencing on multiple device formats. To use this application, a user downloads the application to a computer, mobile phone or other mobile device (*e.g.*, tablet) via direct download from the company's website. Once downloaded and installed, the user is prompted to create an account. "Application A" users can invite others to an online meeting "room," which is an online location associated with a 10-digit number where each user can see and interact with the other users.

8. When a user chooses to enter a specific meeting room, the user enters the 10-digit room number and enters the username that he wants to use on that specific occasion, which does not have to be the same as the account username. "Application A" does not require a certain number of characters for a particular username. Consequently, a user can create a name with a single special character, such as "#" or a single letter, such as "a."

9. During a meeting, users can show a live image or video of themselves to other users through the webcam feature. Users may also display the contents of their own computer desktops to the other users in the room. The ability to display their own computer desktops allows users to show videos and photos to other users in the room. "Application A" also allows users to send text messages visible to all of the users in the room, or private messages that are similar to instant messages sent between two users.

---

[2] The actual name of "Application A" is known to law enforcement and remains active; however, disclosure of the name of the application would potentially alert its users to the fact that law enforcement action is being taken against users of the application, thereby provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, to protect the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the application will be identified herein as "Application A."

10. "Application A" permits users to conduct online video conferences for free for a limited number of minutes. Paid subscribers can conduct online video conferences for an unlimited amount of time. Some "Application A" users with a paid account permit their rooms to be accessed without a password such that anyone who knows the room number can enter and leave the room at any time.

11. "Application A" maintains IP address logs for each meeting room, which includes all of the IP addresses (and related usernames) for each user in a particular room on a specific day and the device that was used by each user. Each user's unique IP address is logged to reflect the time that particular user entered the room and the time the user exited the room. Users can enter and exit the room multiple times, thereby creating multiple sessions[3] within the logs of "Application A." In other words, if a room is open and active for one hour, and in that hour, a user enters the room, leaves the room, and then re-enters the room, the "Application A" IP log records would reflect two sessions for that specific user (entry/exit, followed by second entry) in the same room on that date.

12. As noted above, on March 29, 2021, the OCE while located in Linthicum, Maryland, and using a device connected to the Internet, observed a user in the group "Nepirape" on the Chat Application share a link for the Subject Meeting on Application A. The link included a long string of seemingly randomly generated letters and numbers. The OCE accessed the link and as it was being launched, a window for a video preview appeared and provided the OCE with an option to join the Subject Meeting with or without video. The OCE selected the option to enter without video. Once the Subject Meeting was fully viewable, an additional

[3] As used herein, a session refers to a particular user's time in a specific "Application A" room.

window appeared to request whether to join with computer audio. The OCE selected to disable this feature.

13. After entering the Subject Meeting, the OCE observed that one of the participants in the meeting was sharing his screen through the screen-share function and was streaming CSAM videos to the other participants. The CSAM videos generally depicted the sexual abuse of young boys who mostly appeared to be prepubescent and approximately between the ages of 5-10 years old.

14. Many of the participants in the Subject Meeting appeared to have their cameras turned on and were visible through a series of small windows on the side of the screen. Several the participants whose cameras were on could be seen fully or partially naked, and some of them were visibly masturbating. Many of the display names included the word "perv." Additionally, there was also a chat function within the meeting that allowed the users to communicate with each other. Some of the public comments that were viewable by the OCE throughout the recording included what appeared to be commentary on the streamed CSAM, including "nice boyfuck" "loove being pedo," "great asian boy," "rapeehimm," "rape and no dirty dick?" "I wana feel a boy," and "Just look how much bigger the pedoi is compared to the boy!" During the Subject Meeting, approximately 50-70 participants were observed.

15. One particular participant in the Subject Meeting was an individual with the display name "OHperv," believed to be ZACHARY RYAN BALUSIK (hereinafter "TARGET USER" or BALUSIK). TARGET USER "OHperv" had his camera on and was first visible in the participant window on the right-hand side of the screen around 00:54 seconds of the session that was recorded by the OCE. In the visible portion of the window for this user, he was seen fully naked from the neck down, erect and masturbating while the CSAM or child pornography

was streaming at that time. The video that was streaming to participants—including TARGET USER, "OHperv," after he first appeared—through the screen-share function depicted prepubescent boys, between the ages of 5-10, engaging in anal sex. TARGET USER was seen on screen again around 01:48 seconds. During this time, the video that was streaming depicted two prepubescent boys, between the ages of 5-10, engaging in anal sex. TARGET USER was seen on screen again at 17:10 seconds and during this time, the video that was streaming depicted a prepubescent boy, around the age of 5 being anally penetrated by an adult male. During these video segments of TARGET USER, Affiant noticed two pillows with white pillow covers stacked behind the TARGET USER. Affiant also observed what appeared to be a blue in color bed comforter, blanket, or sheet.

16. Pursuant to legal process by the FBI to "Application A" seeking information about the participants in the Subject Meeting during the time the OCE was present and recording and TARGET USER appeared, "Application A" provided information about the subscribed users, including the following subscriber information for the TARGET USER:

Username: OHperv
External IP: 134.228.218.198:51574[4]

17. The results from the legal process served on Application A revealed that TARGET USER/"OHperv" logged in to this "Application A" room from the following IP

[4] A note included with this information from Application A stated that "This is the public facing IP – the IP we see when a user connects to our server. It could be a residential IP, public wifi, an IP used to conceal a user's identity like a Virtual Private Network (VPN) or TOR exit node. After the colon is the port information." Accordingly, the TARGET USER's public-facing IP address was 134.228.218.198. I know from my training and experience that a "port" in networking is a software defined number associated to a network protocol that receives or transmits communication for a specific service. A port in computer hardware is a jack or socket that peripheral hardware plugs into. In this case that port number is not assigned to any specific service.

address on the dates and times specified: 134.228.218.198 on March 29, 2021, join time 18:28:26:813 through leave time 18:31:51:291.5

18. A query of the American Registry for Internet Numbers ("ARIN") online database revealed that IP address 134.228.218.198 was registered to Buckeye Cablevision, Inc.

19. On July 1, 2021, pursuant to legal process for IP address 134.228.218.198 described in Paragraph 24, Buckeye Cablevision, Inc. provided the following as the subscriber information and address:

Name: Zachary Balusik
Service Address: 5026 Ottawa River Rd., Toledo, OH

20. On February 23, 2022, members of the FBI's Northwest Ohio Child Exploitation and Human Trafficking Task Force executed a federal search warrant authorizing a search of 5026 Ottawa River Rd, Toledo, OH, as well as the person of ZACHARY BALUSIK, and any electronics located at the premises or on his person. During execution of the search warrant at the residence, investigators located two thumb or flash drives in the master bedroom in a drawer containing men's clothing. An on-scene preview of the devices revealed child pornography, including child pornography depicting prepubescent children.

21. On that same date, investigators interviewed BALUSIK outside of his residence. BALUSIK admitted to receiving and viewing child pornography, advising that he began approximately 12-13 years ago in 2009 or 2010. BALUSIK admitted to being user "OHperv" on "Application A" and to accessing links containing child pornography that streamed on "Application A." He stated that he used his cell phone to access it from certain social media applications, which he named, and which Affiant knows requires an internet or Wifi connection.

[5] The date and times provided by "Application A" were in GMT.

BALSUIK also advised that he once he clicked on the link, he was taken to "Application A" where there were several other individuals who shared images and videos of child pornography. BALUSIK stated that he accessed these links to child pornography and viewed that child pornography on "Application A" when he was at his residence at 5026 Ottawa River Road, Toledo, Ohio, as well as on other occasions, from his brother's (Nathan Balusik) house while he babysat for his minor nieces and nephew. Both residences are located in the Northern District of Ohio, Western Division. BALUSIK denied saving or storing child pornography; however, after being advised that devices with child pornography were located during the search of his residence, BALUSIK then said that he forgot he had those.

22. On that same date (February 23, 2022), ZACHARY BALUSIK denied committing hands-on conduct of minors and agreed to take a polygraph examination. During the polygraph examination, he was specifically asked whether he had committed hands-on sexual conduct of any minor when he (BALUSIK) was an adult and he denied doing so. He failed the polygraph examination, meaning that he showed deception when denying committing hands-on sexual conduct of any minor while he (BALUSIK) himself was an adult.

23. BALUSIK confirmed that he was employed as a nurse at St. Luke's hospital in the Toledo area. He stated that he works as a head supervisor a couple days of the week and then works as a charge nurse one day of the week.

24. BALUSIK stated that he was scheduled to travel to Mexico on February 24, 2022, advising that he was traveling with his boyfriend.

CONCLUSION

25. Based on all of the information contained herein, I believe probable cause exists that BALUSIK has committed violations of 18 U.S.C. §§ 2252(a)(4)(B), Possession of and/or

Access with Intent to View Child Pornography, and 2252(a)(2), Receipt and/or Distribution of Child Pornography. As such, there is probable cause to arrest ZACHARY RYAN BALUSIK.

26. Based on all of the above, Affiant respectfully requests that this Court issue a complaint and arrest warrant for ZACHARY RYAN BALUSIK.

Special Agent Alex O. Hunt, FBI

Sworn to via telephone after submission by reliable electronic means pursuant to Crim.R. 41(d)(3) and 4.1, this 24 date of February 2022.

s/Darrell A. Clay
Darrell Clay
United States District Court Magistrate Judge